Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Misplaced / Lost Laptop - September 2008

Department(s) Compiling the Report

Financial Markets

Contact Officer

Date of Incident: 20-Sep-08

Date Incident Detected: 20-Sep-08

Date RM Notified: 24.12.08

Summary description of the incident

One of Financial Markets Laptop computers which was due to be returned at the end of it's lease, was detected as missing from the FM Computing storeroom.

Summary of cause

Not determined.

Brief description of impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational/System downtime ☐
- Financial ☑
- Legal ☐
- Reputational ☐

Description

Financial Markets needed to pay out the residual amount for the laptop as it could not be returned to the Leasing company.

Severity of actual impact

Insignificant

Summary action plan

Re-inforced with the FM Compting team, the importance of keeping the inventory records up to date; that loan register is completed in all cases; and, ensure storeroom is adequatley secured at all times.
Current PC Inventory review procedures will be updated to better reflect the physical asset checking requirements along with the Hardcat comparison during the quarterly tests.

Estimated Completion Date

31-Jan-09

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☑
- Yes ☐ ▶ Please select
  - Controls ☐
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

INCIDENT REPORT

MISPLACED LAPTOP – SEPTEMBER 2008

One of FM's Toshiba Portege M300 laptops (Barcode RBA9000364 and Serial Number – 85026132H) which was due to be returned at the end of its lease in September 2008 has been misplaced.

The laptop was in the FM Computing secure storeroom on 3 September 2008, verified by physical inspection, in conjunction with an FM Computing inventory check.

However, when our replacement laptops were configured in the second and third week of September the misplaced laptop was no longer in the storeroom. Unfortunately, on this occasion, the loan register was not updated so there is no record of whom the laptop was issued to.

On 1 October 2008 an email was sent to all FM and Risk Management users asking them to return all Bank supplied laptops for maintenance by 10 October 2008. On 10 October 2008 a reminder was sent to all users requiring them to bring their laptops in for maintenance. During this process all laptops except the misplaced laptop were verified. The misplaced laptop was not returned to the Bank as part of this process.

Subsequently, on 5 November, the Senior Manager, Technology Services sent an email to all staff in FM and RM requesting they check home and work areas for the missing laptop – there was no response to this request.

Impact

This laptop was at the end of its leasing period and was scheduled to be returned to the leasing company at the end of September 2008. As it could not be returned, Financial Markets is required to pay the residual leasing costs of $897-50.

Risk Register

This incident relates to several risks described in the ID and DM Risk Registers - items ID 34 and DM 35 address RBA assets stored in the computer room not matching GL and/or other inventory records. Item ID 37 relates to theft of physical assets. No further changes are required to the risk registers.

Action Plan

- Following this incident, an email was sent to FM Computing staff to reinforce current procedures to ensure that the loan inventory is updated for all laptops and other equipment.
- FM Computing staff were reminded to ensure that the door to the Storeroom is locked at all times (access to the Storeroom is controlled by the Bank's security card access system and the door automatically locks when it is closed). Security guards check the door is secured as part of their nightly walk through of Level 10.
- Current PC Inventory review procedures will be updated to better reflect the physical asset checking requirements along with the comparison during the quarterly tests.

Technology Services
Financial Markets Group
24 December 2008

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Virus 11 June 2009

Department(s) Compiling the Report

ST, FM

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
11-Jun-09	11-Jun-09	12-Jun-09	22-Jun-09

Summary description of the incident

A number of calls were placed to the ST Service Desk advising of accounts being locked out. 82 user accounts were locked out and an additional 20 system related accounts. The current domain password policy is configured to lockout user accounts after incorrect password attempts. It was found that one workstation was the source of repeated attempts to log in to these accounts with password guesses which were incorrect, resulting in the lockouts. This workstation had out of date anti-virus software.

Summary of cause

A USB flash drive connected to a workstation on the RBA LAN was discovered to have the virus. When the user attached the infected USB drive, the Autorun feature of Windows automatically ran the virus on the USB drive. Even though all workstations were correctly patched, the virus ran. however because of the patching it could not propagate.

Brief description of impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational/System downtime ☑
- Financial ☐
- Legal ☐
- Reputational ☐

Description

82 user accounts were locked out for up to half an hour, resulting in the inability to log on, or if logged on, inability to perform some functions such as browsing.

Severity of actual impact

Minor

Summary action plan

- Ensure all RBA workstations have up to date AV
- Define a process for workstations/laptops when they are added and decommissioned from the network that includes addition/deletion.
- Update procedures for regular version checking
- Develop procedure for regular updating of software, patches and anti-virus on Bank equipment used outside of HO, BRS and the branches

Estimated Completion Date

End July 2009

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☑
- Yes ☐ ▶ Please select
  - Controls ☐
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

Please submit Incident Report to RM Operational Risk

FINAL

VIRUS 11-JUNE-2009

1. EXECUTIVE SUMMARY

On 11 June 2009, a USB flash drive connected to a workstation on the RBA LAN was discovered to have the virus. This was identified after a number of calls were placed to the ST Service Desk advising of accounts being locked out. Investigations showed that a single workstation was attempting to authenticate (logon to the LAN) unsuccessfully with multiple user accounts.

The current domain password policy is configured to lockout user accounts after incorrect password attempts and as a result 82 user accounts were locked out and an additional 20 accounts consisting of generic accounts, service accounts and domain administrative accounts were also locked out. The lockout policy operated as designed.

Once the workstation causing this issue was identified it was immediately unplugged from the network and removed by ST Security for further investigation. Forensic analysis of the workstation identified symptoms that the workstation had been compromised including: event logs being deleted, new services being created, and important services being disabled. These symptoms all correspond to the known behaviour of the virus. behaviour also includes attempts to logon to multiple domain accounts using dictionary techniques.

Further analysis tracked the source of the virus to a USB flash drive that a user had plugged in to the workstation to view personal files. Analysis of the USB flash drive confirmed the presence of virus – the virus was subsequently removed from the USB drive.

The Microsoft Operating System patches had been deployed to all RBA workstations to stop the virus from propagating. is designed to stop this virus from spreading over the network however it **does not** stop the virus from operating locally. Because the virus was executed locally from the USB drive, the operating system patch did not block the virus.

However, it was also found that the version running on the workstation was out of date and did not contain the correct virus signature to detect and delete the virus. Had the version of on the workstation been current, the virus would have been detected and prevented from activating.

The risk in this instance was contained quickly and without major harm to the network. The user accounts that were locked out as a result of the virus being active were identified and all accounts were fixed within approximately half an hour.

2. SEQUENCE OF EVENTS

Event Time	Event Description
11:20am	Calls placed to ST Service Desk (CSD) notifying them of user accounts being locked out
11:25am	Server Systems – ST (SS) contacted to investigate
11:30am	SS disconnect workstation from the RBA LAN
11:41am	Security –ST (SEC) notified by suspicious activity coming from the workstation
11:45am	SEC removed the workstation for further investigation
12:10pm	All user accounts that had been locked out were restored to normal by CSD

3. SYMPTOMS

- User accounts being locked out;
- Multiple login attempts from different accounts from one workstation;

4. IMPACT

- Inability for affected users (i.e. the accounts that were locked out) to login or re-authenticate to the LAN;

5. CAUSE

- Virus introduced by an infected USB flash drive attached to an RBA workstation;
- Autorun feature of Microsoft windows automatically accessed the USB flash drive and ran the virus;
- anti-virus was not up to date on the workstation. The workstation had an old version of which is end-of-life;

6. ISSUES

- s was out of date on the PC affected. The process of keeping the network based repository of PCs and laptops data up-to-date is very manual. This allows discrepancies to occur when checking for successful roll-out of software such as

- RBA users are local administrators to RBA workstations meaning that removable media (USB drives) and software can be installed and viruses can execute with privileged rights;
- A virus can masquerade as a user initiated program and list accounts (the central LAN user information directory) allowing the attempts to logon to any LAN account;
- Autorun is turned on by default on RBA workstations – allowing the running, installation and propagation of the virus;

6.1 RELATED ISSUES

While not contributing to the current incident, the following issues could exacerbate any similar occurrences:

- There is no process in ST to ensure that Bank equipment that is used outside of HO and the branches is kept up to date in terms of patching, software versions and virus signatures. This could allow a Bank PC used externally to be infected and subsequently brought onto the Bank's network;
- FM has their own PC support team who install and generally manage the PCs for FM. There is no common definition of procedures and policies of ST and FM to ensure a consistent PC environment is maintained;

7. RISKS AND REFERENCES TO BUSINESS IMPACT ASSESSMENT

System outages as well as information leakage could cause embarrassment to the Bank as well as material loss to the Commonwealth Government due to the inability of the Bank to perform its functions. There have been major outages, both publicly and privately reported, caused by

ST Risk Register - Reputational Risk – 01 Damage to reputation.

ST Risk Register - Op/Information Technology/Performance Failure – 02 Theft due to inadequate security

ST Risk Register - Op/External/Third party – 24 Theft of sensitive information by 3rd party

It is not envisioned that these risks should be changed or that any new risks be added to the register. The "Operational Risk report - 2008-9" of ST by RM notes that "the risk of theft of sensitive information by a third party" is one of the top risks and has an unacceptable risk rating. It also notes that ST is performing further work to address the risk of unauthorised access through desktop PCs.

The relevant reference from the ST's Business Impact Analysis is the Core LAN Environment to the RBA process (ST-1). The overall criticality of this process is Vital. There are no changes to the Business Impact Analysis as a result of the incident.

8. RECOMMENDATIONS

Stopping similar viruses on the RBA network requires several layers of defence

Long term, as viruses become more sophisticated and targeted, the RBA will need to evolve its policies and technology to deal with non-RBA equipment and software being introduced into the RBA network.

In the short to near term, the following are recommended:

- Confirm all workstations have the latest version of anti-viruses and re-examine daily checking procedures to ensure total coverage;
- Introduce a periodic process to check for consistency that all workstations are patched and have up to date anti-virus
- An additional process be put in place by ST to ensure the current manual updating of the network based repository of PCs and laptops (i.e.) is up-to-date, and all relevant areas of ST are informed when workstations are added or decommissioned. Because the process is manual, there is the chance that some discrepancies will exist;

8.1 RELATED INVESTIGATIONS

In addition, there are several other avenues which will be explored although it is not clear whether they will lead to near term improvements in the risk profile:

- Investigate whether the Autorun service should be disabled on workstations. Technically this is possible, however, the full operational impact would need to be assessed;
- Removal of the ability to install and execute non-authorised software within the RBA environment. This would be likely to require some restrictions on the ability of individual users to install software on their workstations without appropriate authorisation. If viable, ST will look to develop a proposal for consideration by the RMC;
- Investigate the use of on the workstation environment – this technology could identify extraordinary or unusual behaviour on workstations and therefore helps guard against zero day attacks where anti-virus signatures are not available;
- provides access to the network for equipment that meets a designated profile such as updated anti-virus and operating system patch levels. has matured in the last few years, but previous reviews found the technology immature. However in cases such as this

i.e. virus activity due to out of date AV, would have prevented workstations joining the RBA network without up to date patches and anti-virus until they were remediated;

9. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
Ensure all RBA workstations have up to date AV	High	High	End June 2009	Security
Define a process for workstations/laptops when they are added and decommissioned from the network that includes addition/deletion.	High	High	End June 2009	Security/ Desktop Services/ Server Systems/ CSD
Update procedures for regular version checking	Medium	Medium	End July 2009	Security
Formalise responsibilities and consistent policies and procedures to be used by ST and FM support teams	Medium	Medium	End July 2009	
Develop procedure for regular updating of software, patches and anti-virus on Bank equipment used outside of HO, BRS and the branches	Medium	Medium	End October 2009	Security/ Desktop Services
Note to all RBA staff regarding risks with USB drives	Medium	Medium	End June 2009	Security

10. RELATED INVESTIGATIONS

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
ST to investigate disabling "autorun" from all Workstations.	Medium	Medium	End August 2009	Desktop services
ST to test functionality on workstations.	Low	Low	End December 2009	Security
ST to investigate options for restricting software installation and execution.	Medium	Medium	End September 2009	Security
Review the use of technology to restrict workstation access to the LAN	Medium	Medium	End December 2009	Security/ Comms

11. DISTRIBUTION LIST

(Include the names of all persons to whom a copy of the incident report will be sent.)

Name	Name	Name

12. SIGN OFF

Title	Name	Signature
ST Department Head		

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Stolen Laptops

Department(s) Compiling the Report

ST

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
13-Aug-09	13-Aug-09		25-Nov-09

Summary description of the incident

In recent months two laptops have been stolen from the homes of ST staff members.

Summary of cause

Laptops are provided to Bank staff for out-of-hours access and for support. The laptops often remain at the home of staff members for the duration of their support cycle.

Brief description of impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational/System downtime ☐
- Financial ☑
- Legal ☐
- Reputational ☐

Description

Residual value of leased laptops - estimated $2600.

Severity of actual impact

Insignificant

Summary action plan

ST staff reminded not to store Bank material on local hard drives.
Bank material should only be stored on encrypted USBs.

Estimated Completion Date

15 May 2010

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☑
- Yes ☐ ▶ Please select
  - Controls ☐
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

Please submit Incident Report to RM Operational Risk

STOLEN LAPTOPS

1. EXECUTIVE SUMMARY

In recent months two laptops have been stolen from the homes of ST staff members. The total financial cost was around $2600. There is no risk of unauthorised access to sensitive data arising from these thefts.

2. SEQUENCE OF EVENTS

On Thursday 13th August 2009 an RBA laptop barcode RBA2008331 was stolen from the home of whilst he was at work. The theft was part of a general home burglary. Police were called and an event number was allocated.

On Tuesday 8th September 2009 an RBA laptop barcode RBA2006002 was stolen from the home of] whilst he was at work. The theft was part of a general home burglary. Police were called and an event number was allocated.

3. SYMPTOMS

In each case the lost laptop was identified as part of the post home-burglary inventory.

4. IMPACT

In one case the laptop was used for on-call support, while the other was made available as part of the BRS arrangements and for general access for the staff member for working on Bank material from home or while travelling. It is possible, although unlikely, that some recent ST working documents were stored on the computers. Any such documents would not contain material of a sensitive nature.

The laptops had standard software for accessing the VPN but are useless for this purpose without associated authenticating material (i.e. logon, password, VPN token). No logons or passwords were stored on the laptops and the VPN tokens were not stolen.

The Bank carries the financial risk on all such thefts. In general this equates to the pro-rata value of the lease plus some residual. ST has not yet received advice from the leasing company, but it is estimated that to cover both laptops, the Bank will be liable for around $2600 in total.

5. CAUSE

Support laptops are usually kept at the home of the staff member who is currently on-call. Staff who have a laptop as a desktop or for ad-hoc out of hours access, would also leave

their laptop at their homes for various periods (e.g weekends or duration short leave breaks, etc).

6. ISSUES

Issues that have been highlighted by this incident include:

- Risk (not realised in this incident) of unauthorised access to data on equipment removed from Bank premises.

7. RISKS AND REFERENCES TO BUSINESS IMPACT ASSESSMENT

This incident relates to the following risks in the ST Risk Register. There are no changes to the risks as a result of the incident:

- Risk 02 Op/Physical Security/Safeguarding Assets – Theft due to inadequate security.
- Risk 24 Op/External/Third Party – Theft of sensitive information by media or third party.

The incident does not relate to a process in the ST Business Impact Assessment.

8. RECOMMENDATIONS

In this case, no sensitive data is known to have been stored on the laptops but this may not always be the case in future thefts. ST recently updated to the RMC on password protection of hard drives. When the documentation and safe approach are finalised a recommendation for its use across the Bank will progressed. In the interim, all ST staff will be reminded that no Bank material should be stored on the local drives of laptops that are left for periods at home. Where material needs to be stored, ST staff should use a prescribed USB which includes encryption.

9. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
Head of ST to remind staff that no Bank material to be stored on local hard drives.	Low	Med	4 Dec 2009	
ST staff to use encrypted USBs when required to store Bank material away from office.	Low	Med	15 Jan 2010[1]	

10. DISTRIBUTION LIST

Name	Name	Name

11. SIGN OFF

Title	Name	Signature
ST Department Head		

[1] This is an estimated date. As reported to the RMC, the USBs have been tested, but the vendor is yet to provide the final version of their solution.

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Accidental release of sensitive information to external contact

Department(s) Compiling the Report

Economic Analysis

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
23-Sep-09	23-Sep-09	23-Sep-09	30-Sep-09

Summary description of the incident

On 23 September, a staff member in the Regional and Industry Analysis section of EA accidently sent a sensitive internal email to an external contact. The person who received the email was an Administration and Research Assistant to the Chief Economist of an industry association (the RBA regularly speaks to this industry association as part of its business liaison program). After realising their mistake within a couple of minutes, the RBA staff member called the external recipient and asked them to delete the email, to which they agreed to straight away. The external recipient assured the RBA staff member that the information contained within the email would not be disclosed any further.

Summary of cause

Carelessness when sending an email.

Brief description of impact

Please select the relevant impact(s)

Personnel health and safety	☐
Operational/System downtime	☐
Financial	☐
Legal	☐
Reputational	☑

Description

Given the sensitivity of the document released, this incident had the potential to cause reputational damage.

Severity of actual impact

Insignificant

Summary action plan

Discuss with ST options to strengthen external email security arrangements. We could possibly move towards sending emails with only a link to an internal document, and with no actual written information contained in the email (i.e. no abstract).

Estimated Completion Date

12/10/2009

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

No ☑

Yes ☐ ▶ Please select

Controls ☐	Risk Description ☐
Risk Ratings ☐	New Risk ☐

Please submit Incident Report to RM Operational Risk

RISK MANAGEMENT

INCIDENT REPORT: ACCIDENTAL RELEASE OF SENSITIVE INFORMATION TO AN EXTERNAL CONTACT

Description

On the morning of 23 September 2009, an economist in the Regional and Industry Analysis (RIA) section of Economic Analysis Department (EA) accidently sent a sensitive internal email to an external contact. The email contained a 7-sentence summary of an analytical note, and a hyperlink to the full document. While the external recipient could not access the full document, the contents of the abstract were sensitive, and could have caused some reputational damage to the RBA.

The RIA economist was asked to send the email to a select list of internal staff members, but their 'autocomplete' function in Outlook added an external recipient with the same last name as one of the intended RBA recipients. The RIA economist did not check their address list before sending the email. The external person who received the email was an Administration and Research Assistant to the Chief Economist of an industry association (the RBA regularly speaks to this industry association as part of its business liaison program).

Impact

While the *potential* impact of this incident could have been significant, the *actual* impact was small. The staff member quickly recognised his mistake, and called the external recipient and asked her to delete the email, to which she agreed to straight away. I also called the Chief Economist involved to make sure that the contents of the email would not be disclosed any further. The Chief Economist indicated that he was sensitive to the problem and was well aware of the obligation of organisations like his (and the RBA) to ensure that emails received in error are deleted.

Risk Register

This incident relates to Risk 01 in the Economic Group's risk register: 'Op/Information/Disclosure–Accidental/Premature release of information. Improper release of sensitive or classified information.'

There are no changes to the risk as a result of the incident.

Business Impact Assessment

The incident relates to EC-3 Publish Data process in the Business Impact Assessment.

No changes are required as a result of the incident.

Action Plan

EA will liaise with S&T to discuss options for strengthening external email security arrangements. Another idea proposed is that EA sends emails with only a link to an internal document, and with no actual written information contained in the email (i.e. no abstract).

Head of Economic Analysis Department
30 September 2009

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

To be submitted with the incident report.

Title of Incident Report

Assignment of external contact to the wrong distribution list 18-Nov-09

Department(s) Compiling the Report

ST

Contact Officer

Date of Incident	Date Incident Detected	Date RM Initially Notified	Date Report Submitted to RM
18-Nov-09	24-Nov-09	25-Nov-09	8 Dec 2009

Summary description of the incident

On the 18th of November 2009 IN requested the ST Service Desk to add an external contact, . to the IN-Contacts(Media) email distribution list . By mistake ST Service Desk staff assigned this external contact to the wrong distribution list, IN-Media-Office. As the All RBA Staff distribution list is made up of other groups, the external contact was effectively also added to this group. Upon discovery on the 24th of November 2009 was removed from the IN-Media -Office group and added to the right group.

Summary of cause

The Service Desk staff performing this request selected the wrong distribution list from the search results. As the Bank has 982 groups a keyword search is used to select groups. This search produced a list where the IN-Media-Office and the IN-Contacts (Media) were presented next to each other. The wrong group was selected. It was caused by human error.

Brief description of impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational/System downtime ☐
- Financial ☐
- Legal ☐
- Reputational ☑

Description

Potential impact was high as confidential information could have been disclosed to an external contact. All emails sent to the IN-Media-Office or All RBA Staff group were sent to the external contact,
Fortunately, no confidential data was sent using these distribution lists before the error was discovered and corrected.

Severity of actual impact

Minor

Summary action plan

The procedure for adding external contacts to the distribution list was changed to incorporate verification by the Manager, Service Desk and the Requestor and Authoriser from the business area. The request is not to be assigned a completed status until confirmation from the business area is received.
The design of the dialogue box highlighting an external destination of email will also be looked to increase its visibility, but as this is externally supplied, there will be limitations on options available.
To give users the opportunity to remove dormant lists and verify membership of the groups, the feasibility of sending distribution lists periodically to their owners for confirmation (every 3 months) will be investigated.

Estimated Completion Date

30-Apr-2010

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☐
- Yes ☑ ▶ Please select
  - Controls ☑
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

Please submit Incident Report to RM Operational Risk

DRAFT / FINAL

ASSIGNMENT OF EXTERNAL CONTACT TO THE WRONG DISTRIBUTION LIST 18-NOV-2009

1. EXECUTIVE SUMMARY

On the 18th of November 2009 IN requested the ST Service Desk to add an external contact to the "IN-Contacts(Media)" email distribution list in the Nat&Metro Newspapers category. By mistake, ST Service Desk staff assigned this external contact to a different email distribution list ("IN-Media-Office"). The distribution list "All RBA Staff" is formed as an aggregation of other email groups. Therefore, the journalist was also effectively added to "All RBA Staff". The cause was human error. The Service Desk staff member selected the "IN-Media-Office" group which was listed immediately under "IN-Contacts(Media)" on the displayed screen of groups.

The journalist received eight "All RBA Staff" emails, along with two emails intended only for the Media Office. There was a potential risk that very confidential information could have been disclosed to the journalist Fortunately, no confidential data were sent using this distribution list before the error was reported and corrected on the 24th of November 2009.

To minimise the risk of such an error happening in the future the procedure for adding an external contact to the distribution list has been changed in order to incorporate verification by the Manager, Service Desk and confirmation by the Requestor and Authoriser from the business area.

2. SEQUENCE OF EVENTS

Event Time	Event Description
18 Nov 09 15:50	sent an email to the Service Desk requesting be added to the IN-Contacts(Media) email group under the 'Nat&Metro Newspapers' category. sent this email using the RBAInfo email box and cc
18 Nov 09 17:32	Heat call 268995 was lodged by

Event Time	Event Description
18 Nov 09 17:40	first created a new external contact To add this new contact, he then called up the list of email distribution groups, but mistakenly selected which was immediately below the intended distribution group.
18 Nov 09 17:43	sent email notification saying "added" back to
24 Nov 09 11:02	from the Service Desk received a call from stating that is receiving emails sent to the RBA staff and requested that it be investigated.
24 Nov 09 11:16	investigated this problem and found that has been added to the group. She removed him from this group immediately and added him to the email group under the category, as per the original request.
24 Nov 09 14:00	asked to request an urgent report of the specific emails sent to
24 Nov 09 15:00	notified about this incident. notified and asked for it to be investigated.
24 Nov 09 15:15	investigated this issue and provided relevant information to
24 Nov 09 16:00	initiated a revision of the procedure with and
24 Nov 09 17:00	asked to raise awareness within the Service Desk group and requested to proceed with extra caution when adding external contacts. also requested secondary verification of all updates.
25 Nov 09 08:33	provides report of emails received by to the Media Office.
25 Nov 09 9:30	The existing procedure was modified by
25 Nov 09 14:30	This incident and a modified procedure were discussed at the Service Desk group meeting. The procedure was implemented by

3. SYMPTOMS

replied to one of the emails sent to the IN-Media-Office group enquiring as to why he is receiving these emails.

4. IMPACT

Potential impact was high as confidential information could have been disclosed to an external contact. All emails sent to All RBA Staff and the group were sent to the external contact, The emails were sent over the course of one week, spanning an episode of particular sensitivity for the Media Office

Fortunately, no confidential data were sent using these distribution lists before the error was discovered and corrected.

5. CAUSE

The Service Desk staff performing this request selected the wrong distribution list from the search results. As the Bank currently has email groups, the keyword search is used to find an appropriate group. The search produced a list where the and the were displayed immediately next to each other. The wrong group was selected and the add button pressed. The cause of the incident was human error.

6. ISSUES

At the time of the incident the Service Desk procedure for adding external or internal contacts to email distribution lists were the same. The procedure did not provide for secondary verification by other Service Desk staff or confirmation by the business area to mitigate the risk caused by assigning a contact to the wrong group.

7. RISKS AND BUSINESS IMPACT ANALYSIS

This incident relates to the following risk in the ST Risk Register.

- Risk 14 Op/Information/Disclosure – Staff release data belonging to the Bank to third party who is not entitled to see it. Accidental or deliberate internal disclosure or ignorance of legislative requirements eg. Improper use of personal or sensitive information such as payroll.

It is proposed to update ST Risk Register to add following control:

Change procedure for adding external contacts to the distribution list to incorporate verification by Manager, Service Desk and confirmation by Requestor and Authoriser from the business area.

8. RECOMMENDATIONS

It is recommended that the procedure for adding external contacts to the distribution list should be changed to incorporate verification by the Manager, Service Desk. Furthermore, the screen print displaying the distribution list's membership should be sent to the Requestor and Authoriser from the business area. The request is not to be assigned a completed status in the Service Desk system until confirmation from the business area is received.

In addition, the feasibility of sending distribution lists periodically to their owners for confirmation (say every 3 months) should be investigated. While this would not directly assist with the current incident, it would give users an opportunity to remove dormant lists and verify membership.

Finally, the dialogue box alerting users that they are sending an email externally will be looked at to see if it can be redesigned to make warnings more prominent. However, this dialogue box is part of externally supplied software and there will be limitations on what options are available.

9. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
Modification of 'Creation/ Editing of Distribution Lists' procedure	High	1	Completed	
Implementation of modified procedure to provide for secondary checking in Service Desk and confirmation by requesting business area.	High	1	Completed	
Investigate feasibility of periodically sending distribution lists to their owners for confirmation (say every 3 months).	Medium	2	End of April 2010	Senior Manager, Service Management & Desktop Support

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
Investigate redesign of the dialogue box alerting users that they are sending an email externally. During the investigation an implementation timeline will be agreed with vendor.	Medium	2	End-January 2010	Senior Manager Security

10. DISTRIBUTION LIST

(Include the names of all persons to whom a copy of the incident report will be sent.)

Name	Name	Name

11. SIGN OFF

Title	Name	Signature
ST Department Head		

ADDENDUM TO INCIDENT REPORT

Assignment of external contact to the wrong distribution list – 18 November 2009

Reference to Business Impact Analysis assessment

This incident relates to the provision of email services and is covered in ST's Business Impact Analysis – Core LAN environment to RBA process (ST-1). There are no changes to ST's Business Impact Analysis as a result of the incident report.

Systems & Technology Department
8 December 2009